REMARKS

Applicant appreciates the Examiner's review of this application and respectfully requests reconsideration and allowance of the pending claims. Claims 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49, 51-63, 65-77, and 79-81 are pending in this application.

Claim Amendments

Claims 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49, 51-63, 65-77, and 79-81 were previously pending.

Claim 1 is currently amended.

No claims are currently canceled.

No new claims are added.

Pending claims: 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49, 51-63, 65-77, and 79-81.

Rejection of the Claims

Rejections under 35 U.S.C. § 103(a)

Claims 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49, 51-63, 65-77, and 79-81 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,079,018 to Hardy ("the Hardy reference" or "Hardy") in view of U.S. Patent No. 6,453, 416 to Epstein ("the Epstein reference" or "Epstein"). Applicant amends claim 1 and respectfully traverses these rejections.

Claim 1

Applicant amends claim 1 to more particularly point out and distinctly claim the subject matter. The amendment does not narrow the scope of claim 1.

Claim 1, as amended, defines a method of:

> generating first and second random values to allow a signature-generating process to generate a signature and additionally encrypt and decrypt a data block;
>
> digitally signing a first string, wherein the first string includes the first random value; and
>
> generating an encryption key for encrypting the data block by hashing a combination of the digitally signed first string and the second random value.

The method of claim 1 generates first and second random values, digitally signs a string that includes the first random value, and generates an encryption key for encrypting a data block (say a document) by hashing a combination of the digitally signed first string and the second random value.

The Hardy reference does not teach or suggest generating multiple random numbers, signing one of the random numbers, and creating an encryption key by hashing a combination of the signed random number and the other random number.

Indeed, the Hardy reference merely describes a "system and method for generating unique secure values for digitally *signing* documents" (c.f., title of the Hardy reference). The Hardy reference provides a pseudo-random key for use in a digital *signature procedure*. Hardy describes generating a distinct value for the pseudo-random key for each distinct document to be digitally *signed* and ensuring

that the pseudo-random key is as unguessable as the private key being used to *sign* the document (col. 1, lines 9-14).

Next, the Epstein reference also does not teach or suggest generating multiple random numbers, signing one of the random numbers, and creating an encryption key by hashing a combination of the signed random number and the other random number.

Indeed, Epstein merely describes a secure proxy signing device, which encrypts a hash of a document with a private key to form the digital *signature* if the hash of the document has been authenticated (e.g., col. 2, lines 40-48). When combined with the Hardy reference, the Epstein reference does not cure the missing teaching in Hardy to produce Applicant's feature of generating an encryption key for encrypting a data block by hashing a combination of: 1) a digitally signed string containing a first random number; and 2) an additional random number. Hence, the combination of Hardy and Epstein fails to produce an obviousness rejection for claim 1.

Since Hardy and Epstein, either alone or in combination, do not teach or suggest Applicant's elements, Applicant respectfully traverses the rejection, and respectfully submits that claim 1 is patentable over the combination of Hardy in view of Epstein.

Claims 2-7, 9-10, and 13-15

For at least the reasons set forth above with respect to claim 1, Applicant submits that claims 2-7, 9-10, and 13-15 are patentable over the Hardy reference in view of Epstein. Dependent claims contain the language of the claims from

which they depend. Claims 2-7, 9-10, and 13-15 depend directly or indirectly from claim 1. Claim 1 is allowable, therefore, claims 2-7, 9-10, and 13-15 are also allowable.

Claims 3 and 4 define the method of claim 1, further including the option of generating a third random value and including the third random value and its hash in a data block to be encrypted as in the method of base claim 1. After encryption, when the data block is later decrypted, the decrypted third random value and the decrypted hash of the third random value can be compared with a new hash of the decrypted third random value. In this way, the decryption key can be verified by comparing the new hash of the decrypted third random value with the decrypted (former) hash of the third random value.

Since neither Hardy nor Epstein disclose Applicant's elements of including values and hash values in the data block to be encrypted and using these included values and hash values as a verification measure for the decryption key, Applicant respectfully submits that claims 3 and 4 are further patentable over Hardy in view of Epstein over and above the reasons stated above.

Claim 16

Claim 16 defines a computer-readable medium having computer-executable instructions for performing steps that include generating first and second random values, digitally signing a string that includes the first random value, and generating an encryption key based on the digitally signed string and the second random value.

As discussed above with respect to claim 1, neither Hardy nor Epstein, alone or in combination, teach or suggest a feature of generating an encryption key for encrypting a data block, the encryption key being based on a hash of a combination of a digitally signed string containing a first random value; the digitally signed string also being combined with a second random value. Applicant respectfully traverses the rejection, and respectfully submits that claim 16 is patentable over Hardy in view of Epstein.

Claims 17-22, 24-25, and 28-30

For at least the reasons set forth above with respect to claim 16, Applicant submits that claims 17-22, 24-25, and 28-30 are patentable over Hardy in view of Epstein. Dependent claims contain the language of the claims from which they depend. Claims 17-22, 24-25, and 28-30 depend directly or indirectly from claim 16. Claim 16 is allowable, therefore claims 17-22, 24-25, and 28-30 are also allowable.

Claim 31

Claim 31 defines an arrangement that includes first logic configured to selectively hash a first data string, wherein the first data string and the hash of the first data string are to be included in a data block to be encrypted by a signature-generating process; second logic operatively coupled to the first logic and configured to digitally sign a second data string; and wherein the first logic is further configured to generate an encryption key based on a combination of the digitally signed second data string and a third data string.

As discussed above with respect to claim 1, neither Hardy nor Epstein, alone or in combination, teach or suggest a feature of generating an encryption key for encrypting a data block based on a hash of a digitally signed string containing a random value. Thus, Applicant respectfully traverses the rejection, and respectfully submits that claim 31 is patentable over Hardy in view of Epstein.

Claims 32, 35-37, 39-41, and 43

For at least the reasons set forth above with respect to claim 31, Applicant submits that claims 32, 35-37, 39-41, and 43 are patentable over Hardy in view of Epstein. Dependent claims contain the language of the claims from which they depend. Claims 32, 35-37, 39-41, and 43 depend directly or indirectly from claim 31. Claim 31 is allowable, therefore claims 32, 35-37, 39-41, and 43 are also allowable.

Claim 44

Claim 44 defines a method that includes generating first, second, and third data strings; digitally signing the second data string; generating an encryption key for encrypting a data block based on the digitally signed second data string and the third data string; encrypting the data block using the encryption key; and storing the encrypted data block, the second data string, and the third data string.

As discussed above with respect to claim 1, neither Hardy nor Epstein, alone or in combination, teach or suggest a feature of generating an encryption key for encrypting a data block based on a hash of a digitally signed string. Thus,

Applicant respectfully traverses the rejection, and respectfully submits that claim 44 is patentable over Hardy in view of Epstein.

Claims 45-49 and 51-57

For at least the reasons set forth above with respect to claim 44, Applicant submits that claims 45-49 and 51-57 are patentable over Hardy in view of Epstein. Dependent claims contain the language of the claims from which they depend. Claims 45-49 and 51-57 depend directly or indirectly from claim 44. Claim 44 is allowable, therefore claims 45-49 and 51-57 are also allowable.

Claim 58

Claim 58 defines a computer-readable medium having computer-executable instructions for performing steps including accessing from storage first, second, and third data strings, digitally signing the second data string, generating an encryption key based on the digitally signed second data string and the third data string, and encrypting a data block using the encryption key.

As discussed above with respect to claim 1, neither Hardy nor Epstein, alone or in combination, teach or suggest a feature of generating an encryption key for encrypting a data block based on a hash of a digitally signed string. Thus, Applicant respectfully traverses the rejection, and respectfully submits that claim 58 is patentable over Hardy in view of Epstein.

Claims 59-63 and 65-71

For at least the reasons set forth above with respect to claim 58, Applicant submits that claims 59-63 and 65-71are patentable over Hardy in view of Epstein.

Dependent claims contain the language of the claims from which they depend. Claims 59-63 and 65-71 depend directly or indirectly from claim 58. Claim 58 is allowable, therefore claims 59-63 and 65-71 are also allowable.

Claim 72

Claim 72 defines a system that includes a data block to be encrypted by an encryption key; a first device capable of generating the encryption key; a second device capable of digitally signing a string; first logic associated with the first device to generate first, second, and third data strings; second logic associated with the second device to digitally sign the second data string; and at least a part of the first logic further configured to generate the encryption key based on the digitally signed second data string and the third data string.

As discussed above with respect to claim 1, neither Hardy nor Epstein, alone or in combination, teach or suggest a feature of generating an encryption key for encrypting a data block based on a hash of a digitally signed string. Thus, Applicant respectfully traverses the rejection, and respectfully submits that claim 72 is patentable over Hardy in view of Epstein.

Claims 73-77 and 79-81

For at least the reasons set forth above with respect to claim 72, Applicant submits that claims 73-77 and 79-81 are patentable over Hardy in view of Epstein. Dependent claims contain the language of the claims from which they depend. Claims 73-77 and 79-81 depend directly or indirectly from claim 72. Claim 72 is allowable, therefore claims 73-77 and 79-81 are also allowable.

CONCLUSION

Applicant respectfully suggests that claims 1-7, 9-10, 12-22, 24-25, 27-32, 35-37, 39-49, 51-63, 65-77, and 79-81 are in condition for allowance and requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 2-25-05

By: 

Lee & Hayes PLLC
Mark C. Farrell
Reg. No. 45,988
(509) 324-9256 x243